REMARKS

Claim Status

Applicants acknowledge, with appreciation, the indication that claims 4, 9, 20 and 23-27 contain allowable subject matter. Claims 1-4, 9-18, 20 and 22-29 are now pending, with claims 1, 10-18, 28 and 29 being in independent form. Claims 1, 10-18, 23 and 25-28 have been amended. New independent claim 29 has been added. Support for the amendments to independent claims 1, 10-18 and 28 may be found, for example, at paragraphs [0018] and [0078] of U.S. Pub. No. 2007/0192607 (i.e., "the published application). Support for the amendments to dependent claims 25-27 may be found, for example, at paragraph [0078] of the published application. No new matter has been added. Reconsideration of the application, as herein amended, is respectfully requested.

Overview of the Office Action

The title of the invention has been objected to as non-descriptive. The title has been amended. Withdrawal of this objection is deemed to be in order.

The Specification has been objected to as failing to provide proper antecedent basis for the claimed subject matter. Withdrawal of this objection is deemed to be in order, as explained below.

Claims 12, 14, 16 and 18 stand rejected under 35 U.S.C. §101 as directed to non-statutory subject matter.

Claims 1, 2, 10-14 and 28 stand rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 6,845,447 ("*Fujioka*") in view of U.S. Pub. No. 2005/0021479 ("*Jorba*").

Claims 3, 15-18 and 22 stand rejected under 35 U.S.C. §103(a) as unpatentable over *Fujioka* in view of *Jorba*, and further in view of NPL "A Verifiable Multi-Authority Secret Election Allowing Abstention from Voting" ("*Juang*").

Applicants have carefully considered the Examiner's rejections and the comments provided in support thereof. For the following reasons, applicants respectfully assert that all claims now presented for examination in the instant application are patentable over the cited art.

Amendments Address Informalities

According to the Examiner, "claim 1 recites a tracing protocol however applicant's specification paragraph 68 of applicant's original disclosure recites a discrepancy-tracing procedure. Additionally the Examiner notes in paragraph 86 of applicant's specification the Examiner notes that the applicant recites a back-tracing procedure. As such the Examiner notes that it is difficult to interpret applicant's claim 1 tracing protocol".

In response to the foregoing, applicants have amended claim 1 to now recite, *inter alia*, "a signature-tracing mechanism". As explained at paragraph [0018] of the published application, "[i]f the signer has a transcript of a particular signing session then he can identify the signature-message pair resulting from that session: this is termed 'signature tracing'. Conversely, if the signer has available a particular signature-message pair then he can determine the signing session at which this was generated: this is termed 'session tracing'". As further explained at paragraph [0078] of the published application, "[o]nce the misbehaving voter's identifier has been revealed, the signature-tracing mechanism of the fair blind signature scheme is applied so as to identify the data-pair (x_{ij}, Y_{ij}) corresponding to Id_y".

Accordingly, in the fair blind digital signature scheme of the invention, a trusted authority can, if provided with a given signature-message pair, help a signer to determine the specific signing session at which that data pair was generated ("session-tracing"). Similarly, if the trusted authority is provided with the transcript of a signing session, then the trusted authority can identify which signature-message pair resulted from that signing session ("signature-tracing"). It is these sessions and signature-tracing mechanisms that are used in the present invention to established the desired link between the data pair and the signing session in which the data pair was generated.

The specification thus does in fact provide proper antecedent basis for the claimed subject matter, and withdrawal of the Examiner's objection is deemed to be in order.

Patentability of Claims 12, 14, 16 and 18 under 35 U.S.C. §101

The Examiner (at pg. 3 of the Office Action) asserts that:

> [claims 12, 14, 16 and 18 are] directed to [a] "computer program". The Examiner notes that the MPEP states that a "computer program" not resident to some form of "computer readable medium" is considered to be non-statutory subject matter. Additionally the Examiner notes that the "medium" must not contain transitory signals

In response to the foregoing, applicants have amended independent claims 12, 14, 16 and 18 to now recite, *inter alia*, "A computer program stored on a computer memory and executing on a processor…". Support for the computer memory may be found, for example, at the last line of paragraph [0062] of the published application or at pg. 10, line 19 of the specification as originally filed. No new matter has been added. Independent claims 12, 14, 16 and 18 have thus been amended to recite that the computer program is stored on a memory and is executed by a processor, where the memory and processor clearly constitute physical structure.

In view of the foregoing, applicants contend that independent claims 12, 14, 16 and 18 as now amended are directed to statutory subject matter; reconsideration and withdrawal of the rejection under 35 U.S.C. §101 are accordingly deemed to be in order, and notice to that effect is requested.

Patentability of the Independent Claims under 35 U.S.C. §103(a)

Independent claim 1 has been amended to now recite, *inter alia*, the step of "establishing, at a trusted authority apparatus, a link between a data pair (x_i, y_i) comprising said data signal and said digital signature, and a signing session in which said data pair (x_i, y_i) was generated, the fair blind signature scheme permitting establishment of the link via a signature-tracing mechanism included in the fair blind signature scheme, said signature-tracing mechanism enabling the trusted authority to identify, based on a transcript of said signing session, the data pair (x_i, y_i) generated during said signing session". Independent claims 10-18 and 28 have been correspondingly amended. Support for the amendments to independent claims 1, 10-18 and 28 may be found, for example, at paragraphs [0018] and [0078] of U.S. Pub. No. 2007/0192607 (i.e., "the published application). No new matter has been added. The Examiner-cited art fails to teach or suggest this expressly-recited subject matter.

The Examiner (at pgs. 4-5 of the Office Action) has acknowledged that *Fujioka* fails to disclose "permitting establishment of the link via a tracing protocol included in the fair blind signature scheme", and cites *Jorba* for this feature.

Applicants disagree, however, that any proper combination of *Fujioka* and *Jorba* either teaches or suggests applicants' claimed invention as recited in independent claim 1, and correspondingly recited in independent claims 10-18 and 28.

Applicants' claimed invention utilizes a fair blind digital signature scheme in an electronic voting system. It is known to use a blind signature scheme in electronic voting systems. However, applicants' claimed invention implements a **fair blind signature** scheme in an electronic voting system. It is essential to appreciate and understand that a **fair blind signature** scheme is different than a blind signature scheme. They are not the same, and far more than the mere coupling of the word "fair" to the words "blind signature" is required to implement or provide a "fair blind signature" scheme.

As explained at paragraphs [0017] and [0018] of the published application, in an ordinary blind signature scheme the signer cannot identify which signature results from a given signing session. In contrast, in a fair blind signature scheme, the signer can – with the aid of a trusted authority – identify which specific signature-message pair resulted from a given signing session or which particular signing session produced a given signature-message pair. Consequently, when a cast vote is later deemed to be problematic, it is possible in accordance with the present invention to determine which cast vote is at the origin of the problem and to remove that particular cast vote from those that are to be counted.

There is no disputing that *Fujioka* discloses a verification methodology that utilizes a conventional **blind signature** scheme, as the Examiner has acknowledged in stating (at pg. 4) "Fujioka is noted to teach a ***blind signature scheme***". (Emphasis Supplied). Again, a blind signature scheme is **not** a **fair blind signature** scheme.

Jorbas, for its part, fails to the cure the deficiencies of *Fujioka.* Here, again, the Examiner (at pg. 5) asserts that "Jorba is noted to teach a blind signature voting scheme comprising a verification tracing protocol (e.g., tracing protocol) where a link ballot identifier is used for traceability purposes. See Jorba paragraph 123". Thus, under the Examiner-proffered analysis,

Jorba likewise teaches a **blind signature scheme**. With no mention whatsoever in *Jorba* of applicants' claimed **fair blind signature scheme**, it follows that *Jorba* necessarily fails to teach or suggest "the fair blind signature scheme permitting establishment of the link via a signature-tracing mechanism included in the fair blind signature scheme, said signature-tracing mechanism enabling the trusted authority to identify, based on a transcript of said signing session, the data pair (x_i, y_i) generated during said signing session", as expressly recited in independent claim 1 and correspondingly recited in independent claims 10-18 and 28.

More specifically, *Jorba* discloses "a secure electronic voting method and the cryptographic scheme used, specially applicable to remote electronic voting through a communication network. Said cryptographic scheme includes cryptographic protocols and processes which take place before, during and after the voting or poll itself" (see paragraph [0027]). *Jorba* (paragraph [0172]) describes a verification process 214 that is utilized to verify votes or poll results. According to *Jorba*, the verification protocol includes downloading a sub-list of and tracing a correct ballot identifier in the downloaded sub-list. However, the verification protocol of *Jorba* is not a tracing protocol that corresponds to applicants' claimed signature-tracing mechanism. In fact, *Jorba* fails to teach or suggest the use of applicants' fair blind signature scheme. To the contrary, the verification protocol of *Jorba* simply enables a user to verify that the vote that he has cast has been counted in a particular election, by associating a ballot identifier with each vote that is cast. *Jorba* fails to teach or suggest anything whatsoever of the use of a fair blind signature scheme that includes a signature-tracing mechanism that enables a trusted authority to identify the data pair generated during a particular signing session. The combination of *Fujioka* and *Jorba* thus fails to provide a system implementing a fair blind digital signature scheme — including a signature-tracing

mechanism — in an electronic voting system as recited in independent claim 1 and correspondingly recited in independent claims 10-18 and 28.

Applicants' claimed invention is based on the use of **fair blind** signatures in conjunction with a signature-tracing mechanism. As previously explained, a **fair blind** signature scheme involves an additional participant (designated as a "trusted authority") and, through the trusted authority, a signer can identify which signature results from a given signing session. The skilled person finds no motivation in the art to modify the teachings of *Fujioka* and *Jorba* to achieve the methods, advantages and functionality achieved by applicants' claimed invention, absent impermissible hindsight reconstruction based on applicants' own disclosure. Independent claims 1, 10-18 and 28 are therefore deemed to be patentable over *Fujioka* and *Jorba*, each of which merely discloses the use of a conventional blind signature scheme.

By virtue of the above-discussed differences between the recitations of claims 1, 10-18 and 28 and the teachings of *Fujioka* and *Jorba*, and the lack of any clear motivation for further modifying the reference teachings to achieve applicants' claimed invention, independent claims 1, 10-18 and 28 are deemed to be patentable over *Fujioka* and *Jorba* under 35 U.S.C. §103.

New Independent Claim 29

New independent claim 29 includes the subject matter of original independent claim 1 and allowable dependent claim 9. Since dependent claim 9 has been identified as containing allowable subject matter, new independent claim 29 is deemed to be in condition for allowance.

Patentability of Dependent Claims 3 and 22 under 35 U.S.C. §103(a)

The Examiner (at pg. 6 of the Office Action) has acknowledged that the combination of *Fujioka* and *Jorba* fails to teach the subject matter of dependent claims 3 and 22, and cites *Juang* for these features.

Applicants disagree, however, that any combination of *Fujioka*, *Jorba* and/or *Juang* achieves the subject matter of dependent claims 3 and 22. There is nothing in *Juang* to cure the above-noted deficiencies in *Fujioka* and/or *Jorba* concerning the lack of teachings of, *inter alia*, the claim 1 recited fair blind signature scheme including a signature-tracing mechanism.

The combination of *Fujioka*, *Jorba* and/or *Juang* therefore fails to teach or suggest the features recited in independent claim 1, let alone in dependent claims 3 and 22. Dependent claims 3 and 22 are accordingly likewise deemed to be patentable under 35 U.S.C. §103(a) over the combination of *Fujioka*, *Jorba* and/or *Juang*.

Dependent Claims

In view of the patentability of independent claims 1, 10-18 and 28, as well as of new independent claim 29, for at least the reasons presented above, each of dependent claims 2-4, 9, 20 and 22-27 is deemed to be patentable therewith over the prior art. Moreover, each of dependent claims 2-4, 9, 20 and 22-27 additionally includes features that serve to still further distinguish the claimed invention over the applied art.

Conclusion

Based on all of the above, applicants submit that the present application is now in full and proper condition for allowance. Prompt and favorable action to this effect, and early passage of the application to issue, are solicited.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned to facilitate an early resolution of any outstanding issues.

It is believed that no fees or charges are required at this time in connection with the present application. However, if any fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 503111.

Respectfully submitted,
COZEN O'CONNOR

By /Lance J. Lieberman/
Lance J. Lieberman
Reg. No. 28,437
277 Park Avenue
New York, New York 10172
(212) 883-4900

Dated: January 24, 2012